

Quantum Algorithms for Unit Group and principal ideal problem

Hong Wang¹ and Zhi Ma^{1, a)}

Zhengzhou Information Science and Technology Institute, Zhengzhou, 450002, China

(Dated: 2 September 2010)

Computing the unit group and solving the principal ideal problem for a number field are two of the main tasks in computational algebraic number theory. This paper proposes efficient quantum algorithms for these two problems when the number field has constant degree. We improve these algorithms proposed by Hallgren by using a period function which is not one-to-one on its fundamental period. Furthermore, given access to a function which encodes the lattice, a new method to compute the basis of an unknown real-valued lattice is presented.

PACS numbers: 03.67.Ac, 03.67.Lx.

I. INTRODUCTION

Quantum algorithms can be used to realize a sub-exponential or even exponential speed-up over known classical algorithms for some mathematical problems by using Shor's⁹ (Shor 1994) algorithm framework. By extending the notion of period function, Hallgren¹⁰ (Hallgren 2002) showed how to approximate to the period of an irrational periodic function. Moreover, Hallgren applied the proposed technique to compute the regulator of a real-quadratic field and solve the principal ideal problem in polynomial time. Computing the regulator (Regulator Problem) and solving the principal ideal problem (PIP) are interesting not only from a pure mathematical point of view. Buchmann⁶ (Buchmann 1990) and Williams proposed a Diffie-Hellman-like cryptosystem whose security is based on PIP. Thus, if we could solve the PIP, we will break the cryptosystem proposed by Buchmann. We should choose a better cryptosystem if we assume that a large-scale quantum computer can be build.

One small problem which arose during these computations was the choice of the right approximation of natural logarithms. There was no known way to choose the approximation in advance for a given number field, so Schmidt¹ (Schmidt 2005) pointed out that there remains a gap in Hallgren's¹⁰ (Hallgren 2002) algorithm for the quadratic case. Moreover, Schmidt closed a gap left open by Hallgren and generalized Hallgren's work to \mathbb{Z}^r . This generalized framework was then applied to compute the unit group of an algebraic number field. Schmidt's algorithm achieved an exponential speed-up over the best classical deterministic algorithm. The problem was also independently solved by Hallgren^{11,12} (Hallgren 2005, Hallgren 2007) himself. Hallgren computed the unit group, solved the principal ideal problem, and computed the class group, for constant degree number fields, in polynomial time.

More recently, Schmidt² (Schmidt 2009) showed that the regulator problem and the PIP in real-quadratic num-

ber fields can also be solved by using functions which are always periodic but are many-to-one on their fundamental period. They showed that Shor's framework could compute the right period even in such a case with constant success probability.

Inspired by Hallgren's original work, we show that the unit group and the principal ideal problem for constant degree number fields, can also be solved by using functions which are always periodic but are many-to-one on their fundamental period lattice. In this paper, we solve these problems for certain many-to-one functions whose period are irrational and present more efficient algorithms for these problems. The success probability for the unit group problem is $(2^{7r+1}r^{2r})^{-1}$ from Schmidt¹ (Schmidt 2005) and $(2^{3r+3}(r \log \Delta)^r)^{-1}$ from Hallgren¹¹ (Hallgren 2005), respectively. However, the probability from this paper is at least $(100 \cdot (3r)^{2r} \cdot 5^r)^{-1}$, where r is a constant and $\log \Delta \geq r$.

The rest of this paper is organized as follows. In section 2, we give a short overview of the quantum computation and the algebraic number theory. In section 3, a quantum algorithm for computing the unit group of a given number field will be presented. In section 4, we propose an algorithm for the principal ideal problem. Conclusions are given in section 5.

II. BACKGROUNDS

A. Quantum Computing

First we give a brief introduction to quantum computation. Many problems that have quantum algorithms with exponential speed-up over the best known classical algorithm use the quantum Fourier transform (QFT) as a subroutine. These problems can be reduced to the problem of finding a basis of a period lattice Λ . We denote by \cdot the dot product of two vectors and by the lattice Λ^* which is dual to Λ , i.e., $\Lambda^* = \{\mathbf{v} \in \text{span}(\Lambda) \mid \forall \mathbf{u} \in \Lambda : \mathbf{v} \cdot \mathbf{u} \in \mathbb{Z}\}$. Generally speaking, if a basis of the dual lattice Λ^* is known, one can compute a basis of the original lattice Λ by classical computer efficiently. So, it is enough for the quantum algorithms to

^{a)} Electronic mail: fallmoonma@163.com.

find an approximation of a basis \mathbf{B} for the dual lattice Λ^* . Several known quantum algorithms which achieved exponential speed-up are based on this framework, such as Shor's factorization and discrete logarithms algorithms, Hallgren's algorithms for pell's equation.

The framework for such an algorithm proceeds as follows: The quantum computer uses two registers: one to store the input of the function and the other to store the function value. Firstly, the quantum computer creates a superposition of all possible states in the first register, computes the function values and stores them in the second register. Secondly, we measure the second register. By the laws of quantum mechanics, the state of the quantum computer transforms into $\sum_{\mathbf{v} \in L} |\mathbf{u} + \mathbf{v}\rangle |f(\mathbf{u})\rangle$ where \mathbf{u} is a random vector and L is a subset of Λ . Thirdly, the QFT and a measurement are applied to the first register. Now, we get a vector from a basis of Λ^* .

So, for a lattice Λ with fixed dimension, we can get an approximation of the basis \mathbf{B} of the lattice Λ^* with fixed probability after running the subroutine above a constant number of times. The QFT has an interesting and useful property, known as shift invariance. i.e., the resulting distribution is independent of which coset is started with. Thus, the QFT always creates a superposition of value which approximates the basis of Λ^* independent of \mathbf{u} . Furthermore, after running the QFT to the register, the elements in the superposition are almost uniformly distributed. More detail about quantum computing, see Nielsen's⁸ (Nielsen2000) book.

B. Algebraic number theory

In this section we give the necessary background on algebraic number theory. One can find almost all of the following facts from Thiel's³ (Thiel 1995) work or Cohen's⁵ (Cohen 1993) standard book on computational algebraic number theory.

A number field K can be defined as a subfield of the complex numbers \mathbb{C} which is generated over the rational numbers \mathbb{Q} by an algebraic number, i.e., $K = \mathbb{Q}(\theta)$ where θ where θ is a root of a monic irreducible polynomial of degree n with rational coefficients, which is called the minimal polynomial of θ . The number n is called the degree of K (over \mathbb{Q}). The signature of K is the pair $(s, t) \in |\mathbb{Z}| \times |\mathbb{Z}|$, where s is the number of real zeros of the minimal polynomial of θ and t is the number of pairs of nonreal zeros; clearly, we have $s + 2t = n$. The signature is independent of the choice of the generating polynomial and thus is an invariant of the number field.

First we introduce some properties associated with number fields. In the following, we shall always assume that $K = \mathbb{Q}(\theta)$ is a number field of signature (s, t) . If $\theta_1, \dots, \theta_n$ are the roots of the minimal polynomial of θ , then there are n ways to embed the number field in \mathbb{C} . Let $m = s + t$. An element in K has n conjugates, and K has m absolute values, all of which correspond to the embeddings. Given any number $\alpha \in K$, $\alpha = \sum_{i=0}^{n-1} a_i \theta^i$ for

some rational numbers $a_i \in \mathbb{Q}$, let $\alpha^{(j)}$ denote the j -th conjugate of α , i.e., the image of α in the j -th embedding: $\alpha^{(j)} = \sum_{i=0}^{n-1} a_i \theta_j^i$. The j -th absolute value $|\cdot|_j$ of a number α is a function of the absolute value in the j -th conjugate field: $|\alpha|_j = \begin{cases} |\alpha^{(j)}| & 1 \leq j \leq s \\ |\alpha^{(j)}|^2 & s+1 \leq j \leq m \end{cases}$, where $|\alpha|_j = 0 \Leftrightarrow \alpha = 0$.

An order \mathcal{O} of a number field K is a subring of containing 1 that also is a module of K . Let \mathcal{O} be an order of a number field K . A number $\xi \in \mathcal{O}$ such that $\xi^{-1} \in \mathcal{O}$ is called a unit \mathcal{O} . The set of all units of \mathcal{O} is a multiplicative abelian group that is called the unit group of \mathcal{O} and is denoted by \mathcal{O}^* . By Dirichlet unit theorem, if we set $r = s + t - 1$, we see that there exist $\varepsilon_1, \dots, \varepsilon_r$ such that every $\varepsilon \in \mathcal{O}^*$ can be written in a unique way as $\varepsilon = \zeta \varepsilon_1^{n_1} \dots \varepsilon_r^{n_r}$, where $n_i \in \mathbb{Z}$ and ζ is a root of unity in K . So the unit group in general will be isomorphic to \mathbb{Z}^r , together with a root of unity. Given a number field of constant degree, the root of unity can be computed efficiently by a classical computer. So computing the unit group \mathcal{O}^* will mean computing a fundamental system of units $\varepsilon_1, \dots, \varepsilon_r$ that generate \mathcal{O}^* .

Definition 1 A fractional \mathcal{O} -ideal I is a non-zero free \mathbb{Z} -submodule of K such that there exists a non-zero integer d with dI ideal of \mathcal{O} . An ideal is said to be a principal ideal if there exists $x \in K$ such that $I = x\mathcal{O}$.

Definition 2 Let I is a fractional ideal and α a non-zero element of I . We will say that α is a minimum of I if, for all $\beta \in I$, we have $\forall i, |\beta|_i < |\alpha|_i \Rightarrow \beta = 0$, and the set of all minima of \mathcal{O} will be denote by $\mathcal{M}_{\mathcal{O}}$. We will say that the ideal I is reduced if $l(I)$ is a minimum in I , where $I \cap \mathbb{Q} = l(I)\mathbb{Z}$.

For a given ideal, there are an exponential number of minima in general. A reduced ideal is important because it is possible to keep the representation size bounded by a polynomial. The set of all principal reduced ideals $\mathcal{R}_{\mathcal{O}}$ is precisely the set of ideals $\frac{1}{\sigma}\mathcal{O}$ where σ runs through all minima of \mathcal{O} .

Definition 3 The logarithmic embedding of K^* in \mathbb{R}^{s+t} is the map Log which sends α to

$$\text{Log} : \alpha \mapsto (\log |\alpha|_1, \dots, \log |\alpha|_{s+t}).$$

Definition 4 (Unit group problem). Given a number field K and the ring of integers \mathcal{O} , find a system of fundamental units of K .

Lemma 1⁵ (Cohen 1993) The image of the group of units \mathcal{O}^* under the logarithmic embedding is a lattice (of rank r) in the hyperplane $\sum_{1 \leq i \leq s+t} \alpha_i = 0$ of \mathbb{R}^{r+1} . The kernel of the logarithmic embedding is exactly equal to the group of the roots of unity in K .

Given the lattice Λ , one can get the group of unit \mathcal{O}^* by classical computer efficiently. So it is enough for us to find a basis of the lattice Λ .

III. COMPUTING THE UNIT GROUP

A. The periodic function

By assigning to each point \mathbf{v} in \mathbb{Q}^r the element of $\mathcal{R}_\mathcal{O}$ which is closest to $\mathbf{v} \bmod \Lambda$ we obtain a periodic function with period lattice Λ . Unlike Hallgren's work, we consider many-to-one periodic function, thus, stringent injectivity entirely discarded.

First we give the definition of the periodic function on \mathbb{Z}^r hides Λ for computing the unit group. For some $N \in \mathbb{Z}$ we define f_N as follows:

$$f_N : \mathbb{Z}^r \rightarrow \mathcal{R}_\mathcal{O} : \mathbf{v} \mapsto I_{\mathbf{v}/N} = \frac{1}{\sigma(\mathbf{v}/N)} \mathcal{O}$$

Where $I_{\mathbf{v}/N} = \frac{1}{\sigma(\mathbf{v}/N)} \mathcal{O}$ is the reduced ideal such that $\sigma(\mathbf{v}/N)$ is the minimum of \mathcal{O} that minimizes $\|\mathbf{v}/N - \text{Log} \sigma(\mathbf{v}/N)\|_2$. Especially, if there are two or more $\sigma(\mathbf{v}/N)$ meet the condition, we choose the right one by lexicographic comparison.

The difference between function defined by Hallgren's and this paper is that the injectivity in our function will be dropped entirely. By the results of Hallgren¹¹ (Hallgren 2005) and Schmidt¹ (Schmidt 2005), and demonstrated in detail in algorithm 6.2.20³ (Thiel 1995), one can compute the reduced ideal that near the given point in polynomial time for number fields with constant degree.

Next we will show that f_N is periodic.

Definition 5 Let $M \subset \mathbb{Z}^r$, the centre of M is one point $\mathbf{p} \in M$ such that for any $\mathbf{p}' \in M$, $\sum_{\mathbf{v} \in M} \|\mathbf{p} - \mathbf{v}\|_2 \leq \sum_{\mathbf{v} \in M} \|\mathbf{p}' - \mathbf{v}\|_2$, especially, if there are two or more \mathbf{p} meet the condition, we choose the right by one by lexicographic.

Lemma 2 Let $S_\sigma = \{\mathbf{w}' \in \mathbb{Z}_q^r | f_N(\mathbf{w}') = \frac{1}{\sigma} \mathcal{O}\}$ and $\mathbf{v} \in \mathbb{Z}_q^r$ belong to the same fundamental parallelepiped of $N\Lambda$, \mathbf{w} is the centre of S_σ . We denote the absolute of the discriminant of \mathcal{O} by $\Delta_\mathcal{O}$. Then, for any $\mathbf{n} \in N\Lambda$, there exists $\|\beta(\mathbf{w}, \mathbf{n})\|_\infty \leq \frac{1}{4} \log \Delta_\mathcal{O}$ such that the following is true,

- (1) Let $\bar{\mathbf{v}} = \mathbf{v} - \mathbf{w} = (\bar{v}_1, \bar{v}_2, \dots, \bar{v}_r)$, $\beta(\mathbf{w}, \mathbf{n}) = (\beta_1, \beta_2, \dots, \beta_r)$, for any $1 \leq i \leq r$, if $|\bar{v}_i| > |\beta_i|$, then $\mathbf{w} + \bar{\mathbf{v}} + \mathbf{n} + \rho(\mathbf{w}, \mathbf{n}) \notin S_\sigma$, where $\|\rho(\mathbf{w}, \mathbf{n})\|_\infty \leq 1/2$.
- (2) For $\mathbf{n}, \mathbf{n}' \in N\Lambda$, $\max_{\mathbf{n}, \mathbf{n}'} \|\beta(\mathbf{w}, \mathbf{n}) - \beta(\mathbf{w}, \mathbf{n}')\|_\infty \leq 2$.

Proof: (1) By lemma 5.1.14 proved in [9], the number N of minima in a box of side length $\frac{1}{4} \log \Delta_\mathcal{O}$ satisfies $1 \leq N \leq 4^n (\log \Delta_\mathcal{O})^r$. So the distance of two minimum is less than $\frac{1}{2} \log \Delta_\mathcal{O}$, then, if $|\bar{v}_i| > \frac{1}{4} \log \Delta_\mathcal{O}$, we have $\mathbf{w} + \bar{\mathbf{v}} + \mathbf{n} + \rho(\mathbf{w}, \mathbf{n}) \notin S_\sigma$, i.e. $\|\beta(\mathbf{w}, \mathbf{n})\|_\infty \leq \frac{1}{4} \log \Delta_\mathcal{O}$.

(2) Let $\mathbf{n} = N \text{Log} \varepsilon$ for some unit ε . If σ is the minimum closest to $\frac{\mathbf{w} + \bar{\mathbf{v}}}{N}$, then in most of case, $\varepsilon \sigma$ is the one closest to $\frac{[\mathbf{w} + \bar{\mathbf{v}} + \mathbf{n}]}{N}$. Here $[\cdot]$ rounds to the closest integer and is applied to the vector component-wise. If and only if $\mathbf{w} + \bar{\mathbf{v}}$ is in the boundary of S_σ , we can't determine whether $\mathbf{w} + \bar{\mathbf{v}} + \mathbf{n} + \rho(\mathbf{w}, \mathbf{n}) \in S_\sigma$

holds. Then due to rounding, for different $\mathbf{n}, \mathbf{n}' \in N\Lambda$, $\max_{\mathbf{n}, \mathbf{n}'} \|\beta(\mathbf{w}, \mathbf{n}) - \beta(\mathbf{w}, \mathbf{n}')\|_\infty \leq 2$.

B. The algorithm

In this section we present a method to compute a basis for a constant dimensional lattice hidden by a function, and to solve some instances of the hidden subgroup problem over \mathbb{R}^r .

Given a function hiding a lattice Λ we will show how to compute a basis for the dual lattice Λ^* . To compute a basis for Λ we need the lattice be well conditioned. A lattice is well conditioned if a matrix \mathbf{B} whose columns form a basis for Λ is well conditioned, i.e., if $\|\mathbf{B}\| \cdot \|\mathbf{B}^{-1}\|$ is bounded.

We denote the discriminant of K by Δ . For the purposes of analyzing running times, it is customary to use Δ as input, and an algorithm is polynomial or exponential if it is in $O((\log \Delta)^c)$ or $O(\Delta^{c'})$ for some $c, c' \in \mathbb{R}$, respectively, where the O -constants might depend exponentially on n .

Next we propose an algorithm to find an ε -approximation to a basis of Λ^* .

Let $N \gg (\log \Delta)^r$ and $q \gg \det(N\Lambda)$ be a power of 2. Now we present our algorithm. The complete analysis will be given later.

Algorithm 1

Input: Number field K and the ring of integers \mathcal{O}

Out: A set of vectors approximating a basis for $\Lambda = \text{Log} \mathcal{O}^*$

1) (Create superposition)

$$\rightarrow \frac{1}{\sqrt{q^r}} \sum_{w_1=0}^{q-1} \dots \sum_{w_r=0}^{q-1} |w_1\rangle \dots |w_r\rangle |0\rangle;$$

2) (Compute function)

$$\rightarrow \frac{1}{\sqrt{q^r}} \sum_{w_1=0}^{q-1} \dots \sum_{w_r=0}^{q-1} |w_1\rangle \dots |w_r\rangle |f_N(\mathbf{w})\rangle; \text{ where } \mathbf{w} = (w_1, \dots, w_r).$$

3) (Measure the second register)

$$\rightarrow \frac{1}{\sqrt{T}} \sum_{\mathbf{n} \in L} \sum_{i=1}^{\text{vol}(\beta(\mathbf{w}, \mathbf{n}))} |\mathbf{w} + \bar{\mathbf{v}}_i + \mathbf{n} + \rho(\mathbf{w}, \mathbf{n})\rangle |f_N(\mathbf{w})\rangle$$

With a random \mathbf{w} , $T = \text{card} \{\mathbf{w}' \in \mathbb{Z}_q^r | f_N(\mathbf{w}') = f_N(\mathbf{w})\}$, $\text{vol}(\beta(\mathbf{w}, \mathbf{n}))$ is the number of $\mathbf{v}_i = (v_{i1}, \dots, v_{ir}) \in \mathbb{Z}_q^r$ such that $|\bar{v}_{ij}| = |v_{ij} - w_j| < \beta_j$ and $f_N(\mathbf{w} + \bar{\mathbf{v}}_i + \mathbf{n} + \rho(\mathbf{w}, \mathbf{n})) = f_N(\mathbf{w})$; $L = \{\mathbf{n} \in N\Lambda | \mathbf{w} + \bar{\mathbf{v}}_i + \mathbf{n} + \rho(\mathbf{w}, \mathbf{n}) \in \mathbb{Z}_q^r\}$

Test whether $f(\mathbf{w})$ lie in the set for which periodicity can be guaranteed, if not, restart;

4) (Apply the QFT to the first register)

$$\rightarrow \frac{1}{\sqrt{(kq)^r T}} \sum_{\mathbf{c} \in \mathbb{Z}_{qk}^r} \sum_{\mathbf{n} \in L} \sum_{i=1}^{\text{vol}(\beta(\mathbf{w}, \mathbf{n}))} \exp\left(\frac{2\pi i}{qk} (\mathbf{w} + \bar{\mathbf{v}}_i + \mathbf{n} + \rho(\mathbf{w}, \mathbf{n})) \cdot \mathbf{c}\right) |\mathbf{c}\rangle |f_N(\mathbf{w})\rangle$$

Where k is a constant that will be determined later;

5) Measure and return the first register \mathbf{c} ;

- 6) Repeat the procedure; compute a basis of $(N\Lambda)^*$ from the spanning set of vectors;
- 7) Compute a basis for Λ classically.

Notes: We will explain the constant k appearing in step 4. In algorithm 1, just run the QFT over \mathbb{Z}_q^r as usual does not appear to be enough to recover the dual lattice. To overcome this problem we use constant k to run the QFT, i.e. we 'zero-fill', to compute the larger domain \mathbb{Z}_{qk}^r , with the additional part of the domain taking zero values. This constraint also helps us to confine the errors caused by the factor $\rho(\mathbf{w}, \mathbf{n})$ in the function f_N . This type of operation has been studied by Hallgren^{7,11} (Hallgren 2005, Hales 1999).

Algorithm 1 is a typical algorithm for hidden subgroup problem. After apply the QFT and measure the first register, we can get an appropriate \mathbf{c} . Thus, one vector from a basis of $(N\Lambda)^*$ can be efficiently obtained.

Next, we will present the complete analysis for success probability.

We want to estimate the probability to measure \mathbf{c} with $\|\mathbf{c}/qk - \mathbf{n}^*\|_\infty \leq \frac{1}{2qk}$. To keep the influence of disturbing $\rho(\mathbf{w}, \mathbf{n})$ small, we consider only "small" \mathbf{c} and restart the algorithm if \mathbf{c} is too big. For simplify analysis, without loss of generality, let $\beta(\mathbf{w}, \mathbf{n}) = (\beta_1, \beta_2, \dots, \beta_r)$ and $\beta_i = \beta$, ($1 \leq i \leq r$), i.e., S_σ be a multidimensional sphere and β is radius.

Lemma 3 Let $k = 3r$, $\mathbf{c}/qk = \mathbf{n}^* + \delta(\mathbf{c})$,

$\mathbf{C} = \left\{ \mathbf{c} \in \mathbb{Z}_{qk}^r \mid \|\mathbf{c}\|_\infty < \frac{q}{5 \cdot (\beta+1)}, \mathbf{c}/qk - \delta(\mathbf{c}) \in (N\Lambda)^* \right\}$, where $\|\delta(\mathbf{c})\|_\infty \leq \frac{1}{2qk}$, then the probability to get a vector from a basis of $(N\Lambda)^*$ is at least $(100 \cdot (3r)^{2r} \cdot 5^r)^{-1}$.

Proof. The QFT is shift invariant.

So for probability estimation we can assume $\mathbf{w} = \mathbf{0}$. The probability to obtain a $\mathbf{c} \in \mathbf{C}$ is

$$\frac{1}{(kq)^r T} \left| \sum_{\mathbf{n} \in L} \sum_{i=1}^{vol(\beta(\mathbf{w}, \mathbf{n}))} \exp \left(\frac{2\pi i}{qk} (\mathbf{w} + \bar{\mathbf{v}}_i + \mathbf{n} + \rho(\mathbf{w}, \mathbf{n})) \cdot \mathbf{c} \right) \right|^2$$

$$= \frac{1}{(kq)^r T} \left| \sum_{\mathbf{n} \in L} \sum_{i=1}^{vol(\beta(\mathbf{w}, \mathbf{n}))} \exp \left(\frac{2\pi i}{qk} (\bar{\mathbf{v}}_i + \mathbf{n} + \rho(\mathbf{w}, \mathbf{n})) \cdot \mathbf{c} \right) \right|^2 \quad (1)$$

let

$$\begin{aligned} s &= (\bar{\mathbf{v}}_i + \mathbf{n} + \rho(\mathbf{w}, \mathbf{n})) \cdot \mathbf{c}/kq \\ &= \bar{\mathbf{v}}_i \cdot \mathbf{c}/kq + \mathbf{n} \cdot (\mathbf{n}^* + \delta(\mathbf{c})) + \rho(\mathbf{w}, \mathbf{n}) \cdot \mathbf{c}/kq \\ &= \bar{\mathbf{v}}_i \cdot \mathbf{c}/kq + \mathbf{n} \cdot \mathbf{n}^* + \mathbf{n} \cdot \delta(\mathbf{c}) + \rho(\mathbf{w}, \mathbf{n}) \cdot \mathbf{c}/kq \end{aligned}$$

Since $\|\mathbf{n}\|_\infty < q$, $\|\mathbf{c}\|_\infty < \frac{q}{5 \cdot (\beta+1)}$, $\|\delta(\mathbf{c})\|_\infty \leq \frac{1}{2qk}$, we have $s \bmod 1 = \bar{\mathbf{v}}_i \cdot \mathbf{c}/kq + \mathbf{n} \cdot \delta(\mathbf{c}) + \rho(\mathbf{w}, \mathbf{n}) \cdot \mathbf{c}/kq$

$$\begin{aligned} &\leq r \frac{\|\bar{\mathbf{v}}_i\|_\infty \cdot q}{5 \cdot (\beta+1) \cdot kq} + r \frac{q}{2qk} + r \frac{q}{10 \cdot (\beta+1) \cdot kq} \\ &\leq \frac{r}{5k} + \frac{r}{2k} + \frac{r}{10k \cdot (\beta+1)} \end{aligned}$$

From the definition of $\beta(\mathbf{w}, \mathbf{n})$, we know that $2k(\beta + 1) \gg 2k$. So if $k = 3r$, then $s \bmod 1 \leq \frac{7}{30} + \frac{1}{30 \cdot (\beta+1)} \approx \frac{7}{30}$. It follows that the angle between

the vectors $\exp \left(\frac{2\pi i}{qk} (\bar{\mathbf{v}}_i + \mathbf{n} + \rho(\mathbf{w}, \mathbf{n})) \cdot \mathbf{c} \right)$ in Eq.(1) is $[-\frac{7}{15}\pi, \frac{7}{15}\pi]$. So the absolute value of the sum is larger than $\frac{T}{(3rq)^r} |\cos \frac{7}{15}\pi|^2 \approx \frac{T}{100 \cdot 3^r r^r q^r}$; Furthermore, applying Proposition 8.7 in⁴ (Micciancio 2002), we have that $\text{card} \{ \mathbf{n} \in L \} \approx \frac{q^r}{\det(N\Lambda)}$, so $T = \text{card} \{ \mathbf{w}' \in \mathbb{Z}_q^r \mid f_N(\mathbf{w}') = f_N(\mathbf{w}) \}$

$$= \sum_{i=1}^{vol(\beta(\mathbf{w}, \mathbf{n}))} \text{card} \{ \mathbf{n} \in L \}$$

$$\geq vol(\beta - 1) \cdot \frac{q^r}{\det(N\Lambda)}$$

Next we approximate the cardinality of \mathbf{C} , We have

$$\begin{aligned} \text{card} \mathbf{C} &\geq \text{card} \left\{ \mathbf{c} \in \mathbb{Z}_{qk}^r \mid \|\mathbf{c}\|_\infty < \frac{q}{5 \cdot (\beta+1)}, \mathbf{c}/qk - \delta(\mathbf{c}) \right. \\ &\quad \left. \in (N\Lambda)^* \right\} \approx \frac{\det(N\Lambda)}{(3r \cdot 5(\beta+1))^r} \end{aligned}$$

$\frac{vol(\beta-1)}{(\beta+1)^r} \approx 1$. Thus, the probability P to measure a 'good' \mathbf{c} is larger than $(100 \cdot (3r)^{2r} \cdot 5^r)^{-1}$. So we can obtain a vector from a basis of $(N\Lambda)^*$ from \mathbf{c} .

From lemma 2 in¹ (Schmidt 2005), we need only a polynomial repetition of algorithm 1 to get a basis for $(N\Lambda)^*$.

Lemma 4¹ (Schmidt 2005) Let Λ be a lattice of a fixed rank r . Then for $B_1 \in \mathbb{R}$, $B_1 > 10\sqrt{r}\lambda_r(\Lambda)$, there is an algorithm which does the following $O(\text{poly} \log(\det(\Lambda)))$. It samples at most random vectors λ from $\Lambda \cap \{ \mathbf{x} \in \mathbb{R}^r \mid 0 \leq x_i < B_1, i = 0, \dots, r \}$ and outputs with probability exponentially close to one a set of vectors from Λ which generate Λ .

Theorem 1 Algorithm 1 computes the unit group \mathcal{O}^* of a constant degree number field K in quantum polynomial time.

Proof. The probability only depends on the degree of the number fields by lemma 3. So, keep the degree fixed, we need only a polynomial repetition of the above algorithm to get a generating set for $(N\Lambda)^*$, the polynomial time bound is clear from lemma 4.

IV. THE PRINCIPAL IDEAL PROBLEM

Definition 6 (Principal ideal problem) Given an ideal I of \mathcal{O} , determine whether or not it is a principal ideal, and if it is, compute $\alpha \in K$ such that $I = \alpha\mathcal{O}$.

Given a reduced principal ideal $I = \alpha\mathcal{O} = I_\theta$, where $\theta = \text{Log} \alpha$, define the function

$g_N : \mathbb{Z} \times \mathbb{Z}^r \rightarrow \mathcal{R}_{\mathcal{O}}$ by $g_N(a, \mathbf{v}) = I_{a\theta - \mathbf{v}/N}$. The ideal $I_{a\theta - \mathbf{v}/N}$ can be computed efficiently by multiplying I^a and $I_{-\mathbf{v}/N}$. Furthermore, the function g_N has period lattice $\bar{\Lambda}$.

Where $\bar{\Lambda} = \{ (b, \eta) \subseteq \mathbb{Z} \times \mathbb{R}^r \mid b\theta - \eta/N \in \Lambda \}$ and one of its basis is $(1, N\theta), (0, \mathbf{v}_1), \dots, (0, \mathbf{v}_r)$. Here \mathbf{v}_i ($1 \leq i \leq r$) are one basis of the lattice $N\Lambda$. Let $\mathbf{e} = (a, \mathbf{v})$ is a $r+1$ dimensional vector, then we can denote $g_N(a, \mathbf{v})$

by $g_N(\mathbf{e})$. Similarly, we give an algorithm to solve the principal ideal problem.

Algorithm 2

Input: Number field K , the ring of integers \mathcal{O} and a reduced ideal I

Output: $\text{Log} \alpha$ if I is a principal ideal, i.e. $I = \alpha\mathcal{O}$; else ‘not principal’

1) Create superstition and compute function $g_N(\mathbf{e})$,
 $\rightarrow \frac{1}{\sqrt{q^{r+1}}} \sum_{\mathbf{e} \in \mathbb{Z}_q^{r+1}} |\mathbf{e}\rangle |g_N(\mathbf{e})\rangle$

where $\mathbf{e} = (e_1, e_2, \dots, e_{r+1})$

2) Measure the second register

$\rightarrow \frac{1}{\sqrt{S}} \sum_{\mathbf{m} \in \mathbf{M}} \sum_{i=1}^{\text{vol}(\beta'(\mathbf{e}, \mathbf{m}))} |\mathbf{e} + \bar{\mathbf{f}}_i + \mathbf{m} + \omega(\mathbf{e}, \mathbf{m})\rangle |g_N(\mathbf{e})\rangle,$

With a random $\mathbf{e} \in \mathbb{Z}_q^{r+1}$, $S = \text{card}\{\mathbf{e}' \in \mathbb{Z}_q^{r+1} | g_N(\mathbf{e}') = g_N(\mathbf{e})\}$, $\text{vol}(\beta'(\mathbf{e}, \mathbf{m}))$ is the number of such that $|\bar{f}_{ij}| = |f_{ij} - e_j| < \beta'_j$ and $g_N(\mathbf{e} + \bar{\mathbf{f}}_i + \mathbf{m} + \omega(\mathbf{e}, \mathbf{m})) = g_N(\mathbf{e})$; $\mathbf{M} = \{\mathbf{m} \in \bar{\Lambda} | \mathbf{e} + \bar{\mathbf{f}}_i + \mathbf{m} + \omega(\mathbf{e}, \mathbf{m}) \in \mathbb{Z}_q^{r+1}\}$.

Test whether $g_N(\mathbf{e})$ lie in the set for which periodicity can be guaranteed, if not, restart;

3) Apply the QFT to the first register

$\frac{1}{\sqrt{(kq)^{r+1}S}} \sum_{\mathbf{c} \in \mathbb{Z}_{qk}^{r+1}} \sum_{\mathbf{m} \in \mathbf{M}} \sum_{i=1}^{\text{vol}(\beta'(\mathbf{e}, \mathbf{m}))} \exp\left(\frac{2\pi i}{qk} (\mathbf{e} + \bar{\mathbf{f}}_i + \mathbf{m} + \omega(\mathbf{e}, \mathbf{m})) \cdot \mathbf{c}\right) |\mathbf{c}\rangle |g_N(\mathbf{e})\rangle$

4) Measure the first register, return \mathbf{c} ;

5) Repeat the procedure, compute a basis of $\bar{\Lambda}$ pick any two of them, $\mathbf{c} = (c, \mathbf{f}_1)$, $\mathbf{d} = (d, \mathbf{f}_2)$ such that $\text{gcd}(c, d) = 1$;

6) Euclidean algorithm compute the linear combination make the first coordinate equal 1, then we have $(1, \mathbf{u}) \in \bar{\Lambda}$, therefore $\mathbf{u} = N \text{Log} \varepsilon \alpha$ for some ε , where $I = \varepsilon \alpha \mathcal{O}$;

7) Reduce \mathbf{u} modulo the basis of $N\Lambda$, give an optional θ' , if θ' is an approximation of θ , return it, else return ‘not principal’;

Theorem 2 Algorithm 2 works correctly as specified and succeeds with constant probability. The principal ideal problem for a constant number field can be solved in polynomial time by running Algorithm 2.

Proof. Algorithm 2 compute a basis of $\bar{\Lambda}$ is obvious. There is not a unique generator, since $\varepsilon I = I$ for any unit $\varepsilon \in \mathcal{O}^*$. Given any ideal a candidate generator α' can be computed by running the algorithm. Then we can compute $\alpha' \mathcal{O}$ by classical computers efficiently. The result is I if and only if I is principal. Furthermore, from the prime number theorem, the probability to obtain two different non-zero vectors with the first coordinate coprime is at least $1/\ln q$. So we can obtain a correct result with pre-determined probability.

V. CONCLUSIONS

In this paper, we solve two problems in computational algebraic number theory. We have proposed algorithms to compute the period lattice of many-to-one periodic functions, and applied the technique to the computation of the unit group of a finite extension K of \mathbb{Q} . Furthermore, we extend the algorithm to solve the PIP. The algorithm prints a correct result with pre-determined probability. Its success probability can be arbitrarily increased by repeating the algorithm. Thus the algorithm can be applied to attack crypto-systems that rely on the difficulty of the principal ideal problem yielding a better idea about which parameter sizes for these crypto-systems remain secure in the presence of quantum computers. This is due to the facts that the function value is a reduced ideal and not a pair of an ideal and a distance.

Here we will discuss a few more open problems. The main problem is that we haven’t attempted to minimize the influence of the degree of number field on the run-time which is unavoidably exponential now. It is still an open problem whether or not there exist quantum algorithms that solve these problems for arbitrary degree number field. The other problems will be computing the class group for a given number field by many-to-one function. Furthermore, finding another practical problem which realize a exponential speed-up by the proposed technique is more challengingly.

¹Arthur Schmidt and Ulrich Vollmer, Proc. of the 37th STOC(ACM, Baltimore, MP, 2005), pp.475-480.

²Arthur Schmidt, Quantum algorithms for many-to-one function to solve the regulator and the principal ideal problem, arxiv:quant-ph/0912.4807, 2009.

³Christoph Thiel, On the complexity of some problems in algorithmic algebraic number theory, PhD thesis, Universität des Saarlandes, Saarbrücken, Germany, 1995.

⁴D. Micciancio and S. Goldwasser, Complexity of Lattice Problems: a cryptographic perspective, The Kluwer International Series in Engineering and Computer Science (Boston, Massachusetts, 2002), Kluwer Academic Publishers, volume 671.

⁵H. Cohen, A course in computational algebraic number theory, volume 138 Graduate Text in mathematics. (Springer-Verlag, 1993)

⁶Johannes Buchmann and Hugh C. Williams, A key-exchange system based on real quadratic fields, Advances in Cryptology - CRYPTO '89 (Gilles Brassard), Springer-Verlag, vol.435 of LNCS, pp.335-343.

⁷L. Hales and S. Hallgren, Proc. of the Thirty-First STOC(ACM, Atlanta, 1999), pp.330-338.

⁸M. Nielsen and I. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, 2000.

⁹P.W. Shor, Proc. of the 35th FOCS (IEEE, New York, 1994), pp.124-134.

¹⁰Sean Hallgren, Proc. of the 34-th Annual STOC(ACM, Montreal, Quebec, Canada, 2002), pp.653-658.

¹¹Sean Hallgren, Proc. of the 37th STOC(ACM, Baltimore, MP, 2005), pp.468-474.

¹²Sean Hallgren, Polynomial-time quantum algorithms for pell equation and the principal ideal problem, Journal of the ACM, 2007, 54(1).